Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 45 (2015) 696 – 705

Procedia Computer Science

International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

A Contemporary Solution to Ferret Out and Obviate the Fake Messages in Vehicular Ad Hoc Networks by not Percolating through Web Server

R.V.S.Lalitha[a], Dr.G.JayaSuma[b]

[a]*Department of C.S.E.,Sri Sai Aditya Institute of Science and Technology,Surampalem,India.*
[b]*Department of I.T.,JNTUK-University College of Engineering,Vizianagaram,India*

Abstract

Ad hoc networks are suitable for wide range applications like battlefields, analyzing traffic and during disaster recovery operations. With the development of Vehicular Ad hoc Networks the transmission of emergency messages is considerably progressed to accelerate traffic safety measures. As vehicles communicate with each other by connecting through Internet and by using Road Side Units (RSI), there will be each and every possibility to transmit fake messages by accessing VANET Server by unfair means. This requires attention of filtering of messages before transmission over the network through the Server. In this paper, the proposed approach provides a magnificent solution in identifying and obstructing fake messages before passing through the Server. This leads to attempt a contemporary approach in blocking fake messages that helps in causing unwanted disturbance to the traffic instantly. In addition to that the intended process gives a clear analysis in storing of the sender along with the timely analysis of message transmission for tracking source. Obviously this outperforms in trusting the alerts of post-crash notifications and reducing security issues in VANETs.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

Keywords: VANET, Security, SPAM messages

1. Introduction

Previously VANETs communicate with others by using in-built circuitry (On Board Unit) that facilitates Short Message Service (SMS) using AT (Attention) commands. Usually mobile phone manufacturers may not implement all AT commands in mobile phones. GSM/GPRS modems have better support for AT commands than ordinary mobiles.

Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).
doi:10.1016/j.procs.2015.03.134

Hence, linking VANET communication with the existing GSM communication provides effective transmission. VANETs is a form of Mobile Ad hoc Network(MANET) that adapt emerging methodologies such as WiFi, IEEE 802.11 b/g, WiMax IEEE 802.16, Bluetooth, IRA, ZigBee for easy and convenient transmission of emergency messages. In order to make roads safer, wireless technologies play vital role in transmitting messages. VANETs communicate with the nodes in their networks using RSIs. VANET is a form of MANET to provide communication between them and between the vehicles and RSIs. If the communication is established directly between the vehicles, it is V2V Communication. On the other way if the communication is between the Vehicles and RSIs then it will be Vehicle to Infrastructure (V2I) or Infrastructure to Vehicle (I2V). These networks provide wide applications like Lane Change Assistance, Road Feature Notifications (eg. downhill curve).

In this network, nodes are vehicles and needs link to nearby vehicles within the range. The problem with the VANET is disruptions occur in the low density zones and congestion occurs in the high density regions. Hence node position is the important parameter of the VANET. By tracking node positions, we can develop the location tracking system and can reduce the possibility of car accidents that cause abnormal loss to human lives. As it is the communication between the vehicles topology changes very frequently. Also it depends on vehicle speed and dynamic path chosen. As far as the reliability concerned, the trusting of messages is a challenging problem. Due to latency, some of the messages transmitted over time creates ambiguous situation to drivers in believing them. Segregation of Genuine messages among communicated messages is very typical. In practical all the messages will be broadcasted irrespective of whether they are real time or not. This leads to haphazard communication in VANETs. So it requires a mechanism that provides a firewall to fake messages, failing which authentic communication is impossible. The primary goal is to identify the fake messages and to prevent them in transmission over the network for not causing unwanted disturbance to traffic. In this paper, how blocking of fake messages is done at the Web Server is discussed.

The rest of the paper is organized as follows. First, Section 2 describes about the preliminary applications done in providing security to VANETs. V2V communication without filtering of fake messages is addressed is Section 3. An analysis of detecting, tracing and blocking of fake messages at the server is done in Section 4. Discussion of rate of transmission of Genuine Vs Fake message transmission is listed in Section 5. Finally, Section 6 concludes about the tracking of node positions time of transmission of genuine/fake messages transmitted which are useful in post investigations.

2. Related Work

Ghassan Samara et al discussed about attacks and threats that occur in VANETs using Vehicular Public Key Infrastructure (VPKI). As encryption and decryption process is time consuming process, emergency messages can be transmitted using “Certificates on Shelf” [3] whose life span is very less usually 1 min. Sometimes vehicular users’ certificates will be outdated. In such cases Certificate Revocation Lists (CRL)[2] takes time for revocation. So an instant mechanism is required to authenticate the user information/user for delivering emergency information.

Gongjun Yan et al addressed a novel approach to provide Global Security by comparing the radar information, traffic information and neighbor information. This solution merely provides solution to Sybil attacks [1],[4][6]. This could be optimum based on the significance of the information trusted. This work might help in detecting false positions of the vehicles as it uses radar information. As this solution is linked up with the line of sight of the radar a solution that detects exact identification of the source is solicited.

Rizwanul Karim Sakib et al proposed a framework to monitor message authentication by Certificate Authority (CA)[4],[8]. The discussion is about how the messages that are arriving at Base Station are monitored by monitoring center before transmission over the network. Emergency messages require rapid checking at the Base Station itself rather redirecting the information to someone for checking. In this paper, selective measures are taken by trapping the Location Information and device id of the user for tracing source. This alerts the user not to misuse the network for illegal operations.

3. V2V Communication

V2V communication is one of the components of Intelligent Transportation System (ITS). The communication can be either between Vehicle to Vehicle (V2V), Vehicle to Road Side Unit (RSU) to (V2I) or between RSU to Infrastructure

to Vehicle(I2V). In V2V communication range is considerably less(~1-10m) if we use On Board Unit(OBU) for sending Short Message Service(SMS). As V2V communication is short range communication, it uses existing Global System for Mobile Communications(GSM) to send messages to farthest nodes for enabling merging of local networks with global networks to give appreciable results. As Location Information(Latitude and Longitude positions on the Geographic earth) is essential for Vehicular networks, linking VANETs with GPRS(General Packet Radio Service) enabled devices and Android mobiles provides abundant communication techniques in transmitting and receiving information over VANETs.

3.1. VANET Architecture

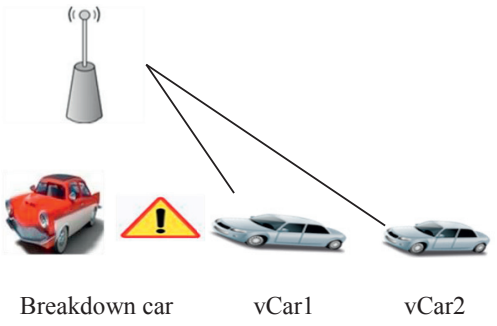


Fig. 1. VANET Architecture
(Existing Communication using GSM)

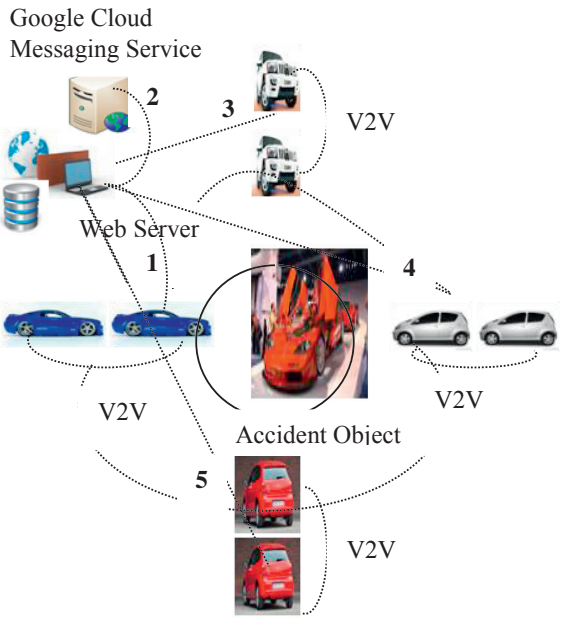


Fig.2. VANET Architecture
(Adapted Communication using GCM Services)

VANET Architecture shown in Fig.1, uses GSM (Global System for Mobile Communications) for communicating with other vehicles. During emergency situations like accidents, drivers communicate with other vehicles using GSM communications. The communication takes place only with the people with people known to them for rescue operations. It could be better, if we are able to send the information to all nearby users who are all disturbed in the accident zone. This leads to an investigative approach to adapt a VANET architecture that has a Web Server to monitor and scrutinizing the messages and using GCM services to pass information both nearer and farthest nodes. This is shown in Fig.2. In this V2V communication takes place via Web Server where messages are monitored. For sending messages to other users on network, the user needs to authenticate with the Web Server and then Web Server uses GCM services to transmit this information to all the nearby vehicles. The functionality of the Web Server in refining the V2V communication is articulated as follows.

3.2. V2V communication without filtering of fake messages

During the case of mishaps, the users send messages to the other vehicles, by passing information to Web Server. The Web Server in turn sends this information to all the VANET users nearby using Google Services. While transmitting data over network no corrective measures are adapted and the information is transmitted as such.

The communication mechanism used in this paper is as follows:-

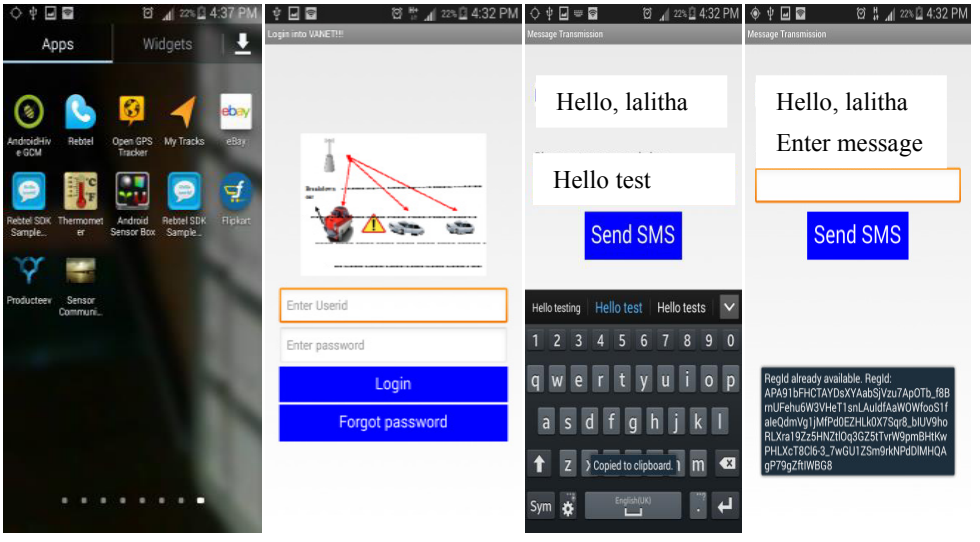
- Users have to add into the network for sharing information across the VANEs.
- Users are authenticated by giving login id and password by the Web Server.
- Only authenticated users are allowed to send information across VANETs.
- All the messages need to be transmitted and received through Web Server only.
- The details of user information like device id, Location Information are also stored in the database for post investigation if required.

3.3. Algorithm Existing Communication Across VANET {

Prerequisites:

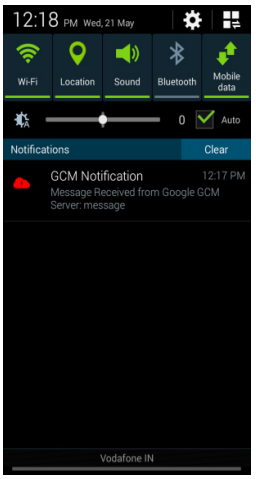
//VANET App is to be installed in the Android mobile.
//Configure Wi-Fi hotspot to access Web Server
//Only authenticated users can transmit messages across network.
//The messages received along with device id will only be transmitted across the network.
Step 1: Login to the application
Step 2: Send message to the Web Server to transmit it over the network.
Step 3: The message along with device ID, latitude and longitude positions will be stored in the Web Server.
Step 4: Web Server can view the source position(Latitude and Longitude) and also all the near by users.
Step 5: Web Server transmits this message over network by using Google Cloud Messaging service provided by GSM.
}

The simulation is done in Android mobiles as follows:-



(a) (b) (c) (d)

Fig.3. a) Android Application b) Login to the VANET
c) Send SMS d) Messaging along with device id



(a)

VANETS

Manage Messages | View Users | Spam Graph | View All Points | Log Out

MESSAGE ID	USER NAME	LONGITUDE	LATITUDE	MSG TIME	
47	lalitha	45.00	30.00	2014-05-24 16:55:0	View on map
46	lalitha	81.78243660977543	17.00825139415025	2014-05-24 16:32:57	View on map
45	lalitha	81.78173882668271	17.00878502902726	2014-05-24 16:30:36	View on map
43	lalitha	80.67435623100123	18.00858502902826	2014-05-24 16:28:36	View on map

(b)

Fig. 4 Reception of messages (a) Viewing message (b) Details of messages transmitted stored in web

Fig.3.(a) is an android application to access Web Server for transmitting emergency messages. To transmit the information over VANET, one has to register as a VANET user as shown in Fig.3.(b). After authentication is verified by the Web Server, the user can send the message to Web Server for transmission over VANET as in Fig.3 (c). While storing the messages in database by the Web Server, the device id is also stored in Web Server in background without the intervention of the user for tracking in post stages if required. This is shown in Fig. 3(d). Finally, the message is transmitted over VANET to all nearby users and can be viewed in their mobiles as a GCM notification as shown in Fig. 4(a). The details of the messages transmitted are stored in Web Server as shown in Fig. 4(b).

The problem with this communication mechanism is anybody can track the web URL and send the information over network which is a bit extravagant. To overcome this situation, to restrict the users transmitting fake messages over VANET, our work suggests an adaptive approach that blocks messages at server.

4. An analysis of detecting, tracing and blocking of fake messages at the server

The prerequisite for transmitting messages over the VANET is the users need to launch the android application in their android mobiles. Also, it is required that all the messages are to be transmitted through Web Server alone. In real mode, the messages are transmitted by choosing Location Information of the intended users. The Web Server checks for authentication, distance, date and time of transmission Location Information and the type of transmission i.e. either

from the mobile or by accessing web URL from mobile. In both the cases the device id is stored in background, thereby allowing the messages to be transmitted over the network.

4.1. In real mode the message transmission is allowed in the following manner:-

- ☑ Administrator alone can transmit the messages from the Web Server
- ☑ Users need to either access the Web Server from their mobiles or can launch android application on their mobiles for message transmission. In either of the cases, since the device id is stored along with the message in background the message transmission is appropriate.
- ✖ If the authenticated user himself accesses the Web Server and sends the message, then as the device id is not stored, the message is treated as "SPAM" and is not allowed to transmit over the network.

4.2. Message Transmission by the Administrator at by tracing of user locations

Since the message transmission from the Web Server is range based, the Web Server monitors and updates user positions on Google Earth after every 20sec.

VANETS

Manage Users View Messages Spam Graph View All Points Log Out

NEW USER REGISTRATION

NAME	USER NAME	LONGITUDE	LATITUDE	LAST LOGIN TIME	
sarath	sarath	81.7825276	17.00085928	2014-05-14 11:21:25	DELETE
chaitanya	chaitu	81.78255633	17.0085605	2014-05-15 11:17:36	DELETE
vijay	vijay	81.7825626	17.0088227	2014-05-21 12:30:36	DELETE
lalitha	lalitha	81.7833505350034	17.00923584258	2014-05-24 13:42:36	DELETE

Fig. 5. User Positions viewed by Web Server

4.3. Particulars of messages stored in Web Server

The Web Server can view the source node on the Google map if required. This allows the identifying passive node communication.

VANETS

Manage Users View Messages Spam Graph View All Points Log Out

NEW USER REGISTRATION

MESSAGE ID	USER NAME	LONGITUDE	LATITUDE	MSG TIME	
47	lalitha	45	30	2014-05-24 16:55:25	View on map
46	lalitha	81.7824366097754	17.008594124	2014-05-24 16:32:36	View on map
45	lalitha	81.78173456897	17.007853445	2014-05-24 16:30:36	View on map
44	lalitha	81.7817384567	17.00978762258	2014-05-24 16:30:36	View on map

Fig.6. Monitoring of messages and viewing of individual user on the Google map in the Web Server

4.4. Viewing of all user positions from the Web Server

For analyzing VANET size the Web Server checks out the all the user positions on the Google map whether they are low density/high density based.

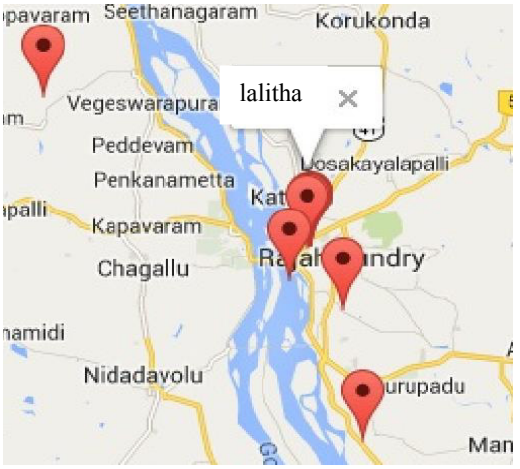


Fig. 7. All user positions on the Google Map

Fig.8. Viewing of individual positions by the Web Server

4.5. Intended user Location Information viewed by the Web Server

The Web Server can view the individual user positions on the Google Earth to trace out the information about origin of message. Also the Web Server finds out the all user positions at the accident spot and updates Location Information for the assessment current position.

5. Detection of Fake message transmission by accessing web URL by the authorized user

There are subtle situations that misfeasors may login to the application for misusing the system. This is illustrated in Fig.8. If this happens, as the device id is not found these messages will be stored by setting the attribute SPAM=”yes” in the database as shown in Fig.9. The main goal of this paper is to avoid this sort of false communications.

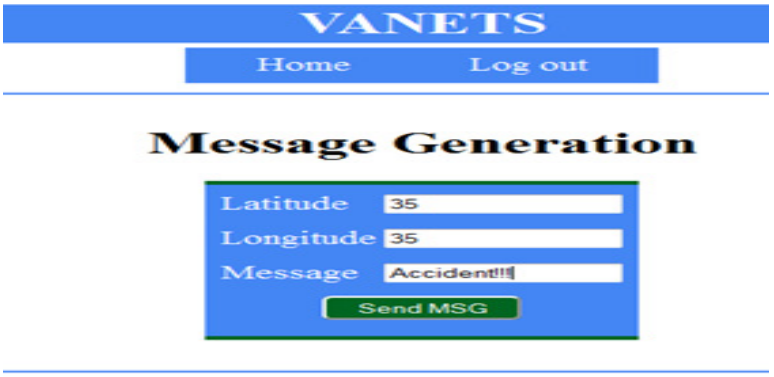


Fig.9. Fake message transmission by accessing Web Server by the misfeasor

VANETS

Manage Users | View Messages | Spam Graph | View All Points | Log Out

NEW USER REGISTRATION

MESSAGE ID	USER NAME	LONGITUDE	LATITUDE	SPAM	MSG TIME	
47	lalitha	45	30	no	2014-05-24 16:55:25	View on map
46	lalitha	81.7824366097754	17.008594124	yes	2014-05-24 16:32:36	View on map
45	lalitha	81.78173456897	17.007853445	no	2014-05-24 16:30:36	View on map
44	lalitha	81.7817384567	17.00978762258	no	2014-05-24 16:30:36	View on map

Fig.10. Blocking of fake messages at by treating them as SPAM=”yes”

6. Detection, tracing and blocking of fake messages at by treating them as SPAM as the device id is not stored in the Web Server

For detection and tracing, Location Information is obtained by viewing the user position as shown Fig.8. The identified messages for which SPAM attribute is set to “yes” are blocked as shown in Fig.10. The no. of genuine/fake messages transmitted on each day is understood with the following graph. This will be helpful in real time analysis for detecting and prevention of transmitting messages over the network.

6.1. Communication across VANETs(Adapted Approach){

Step 1: Login to the application
Step 2: Send message to the Web Server to transmit it over the network.
Step 3: The message along with device ID, latitude and longitude positions will be stored in the Web Server.

Step 4: Web Server computes the distance between it and the origin of message. If the distance is less than 100 the message will be transmitted else not. Go to Step 9.

Step 5: The attribute for the message received along with device ID are set as "NO" and if at all any message received without device ID will be set as "YES".

Step 6: The messages with the attribute set as "YES" will be transmitted as SPAM and are blocked. Go to Step 9.

Step 7: Web Server can view the source position(Latitude and Longitude) and also all the near by users.

Step 8: Web Server transmits this message over network by using Google Cloud Messaging service provided by GSM.

Step 9: End

}

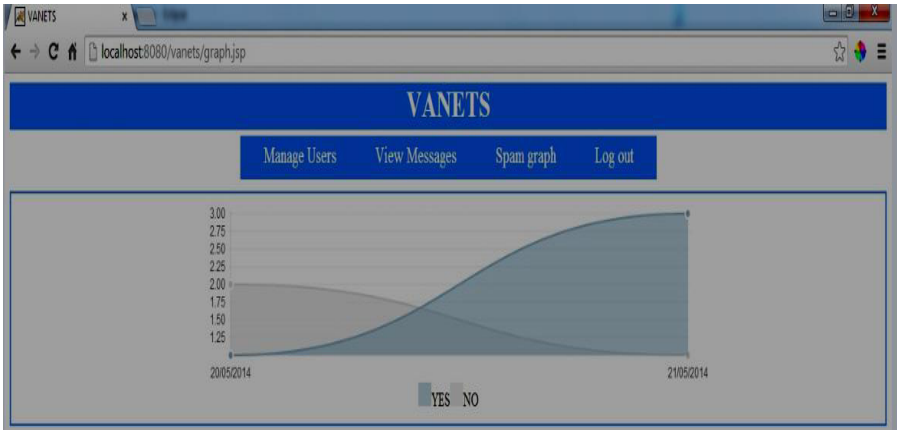


Fig.11. Analysing SPAM/Genuine messages by the Web Server

Conclusions

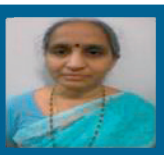
V2V communication sometimes creates adversary effects if fake messages are transmitted. Cookie information and session information stored in web browser leads to this sort of unnecessary confusions and sometimes it may costs to human lives also. This paper presented a vital solution to VANET users by not allowing them to pretend as legitimate user by accessing Web Server. In this paper, the accessing the Web Server by the authenticated user and sending false information to the users is prohibited. As mobile communications are flexible in usage these precautionary measures helps in deriving accurate results in tracing the misfeasors. Still, it is required to stop users from transmitting unwanted messages by crosschecking their profiles at the time of registration itself. As now a days usage of Android mobiles is emerging, it finds ease in implementing the solutions for which Location Information is the prerequisite.

References

1. [2013]Maria Elsa Mathew et al,*Threat Analysis and Defence Mechanisms in VANET,*School of Information Technology and Engineering, VIT University,India.
2. [2013] Ram,Shringar Raw et al, *Security Challenges, Issues and Their Applications for VANET* ,Ambedkar Institute of Advanced Communication Technologies and Research, New Delhi,India.
3. [2010]Ghassan Samara et al, *Security Issues and Challenges of Vehicular Ad Hoc Networks(VANET)*,National Advanced IPv6 Center, University Sains Malaysia.
4. [2005]Krishna Sampigethaya, *CARAVAN:Providing Location Privacy for VANET*, Department of Electrical Engineeri ng, University of Washington, Seattle, WA 98195-2500, University of Tokyo, Tokyo, Japan.
5. [2010]Rizwanul Karim Sakib et al, *Security Issues in VANET*, Department of Electronics and Communication Engineering, BRAC University, Dhaka, Bangladesh.
6. [2008]Gongjun Yan et al, *Providing VANET security through active position detection*, Department of Computer Science, Old Dominion University, Norfolk, VA 23529-0162, USA, [Elsevier].

7. [2007]Gayathri Chandrasekharan et al,*VANETs: The Networking Platform for Future Vehicular Applications, Department of Computer Science, Rutgers University.*
8. [2007]Valentina Casola et al, *An Interoperability System for Authentication and Authorization in VANETs*
9. [2007]Robert K. Schmidt et al, *Vehicle Behavior Analysis to Enhance Security in VANETs,*Institute of Media Informatics, Ulm university, Germany.
10. [2007]EM Van et al,*A Survey of Propagation Models used in Vehicular Ad hoc Network (VANET) Research,*Faculty of EEMCS, The Netherlands.

About the Authors



R.V.S.Lalitha is currently working towards her Ph.D in JNTUK-University College of Engineering, Kakinada. Her research includes Mobile Computing and Soft Computing.

Dr.G.Jaya Suma is H.O.D and Associate Professor in the Department of Information Technology, JNTUK - University College of Engineering, Vizianagaram. She received her Ph.D from Andhra University in 2011. Her current research includes Data Mining, Soft computing and Mobile Computing.